iea

CULTURAL AFFAIRS

VICTORIA HEWSON

May 2021

Paper 1

MORE HARM THAN GOOD?

The perils of regulating online content

IEA papers are designed to promote discussion of economic issues and the role of markets in solving economic and social problems. As with all IEA publications, the views expressed are those of the author and not those of the Institute (which has no corporate view), its managing trustees, Academic Advisory Council, or other senior staff.

Contents

About the author

Victoria Hewson is Head of Regulatory Affairs at the Institute of Economic Affairs. A practising solicitor, she has specialised in commercial, technology and data protection matters across a range of sectors. She has published a number of papers for the IEA including 'Under Control - What HMRC can do to prepare and optimise customs processes for all outcomes' and 'Freedom to Flourish - UK regulatory autonomy, recognition, and a productive economy'. She writes regularly for *The Telegraph* and *City AM* and appears on television and radio to discuss trade and regulatory policy.

Summary

- Online communication and sharing of user generated content have become part of everyday life, but have long worried governments, which have sought to monitor and gain access for reasons of security and crime prevention.
- Until recently, digital platforms were considered to be socially beneficial, and legal measures were passed in jurisdictions including the EU and the United States to facilitate the hosting of user generated content.
- Governments are increasingly worried about what they consider to be the 'harmful' content that is widely available through digital platforms. It has been claimed that democratic processes have been subverted by online disinformation and misinformation, and that children and even adults are at risk of psychological harm and exploitation from offensive or inappropriate material.
- Measures are being pursued to counter these perceived harms, including the EU's Code of Practice on Disinformation and the UK government's forthcoming Online Safety Bill.
- This paper considers the need for such measures and the risks of unintended consequences.

Introduction

Communication of ideas and information is now overwhelmingly done electronically, whether user-generated or editorial, publicly shared on social media or privately shared by direct messages or file sharing. The reach and decentralised nature of online communications have long worried governments, which are concerned about terrorists, child abusers and other criminals using the internet to plot and execute their activities. There have been legal battles as security services sought access to private communications and data through surveillance and data retention obligations on service providers, resisted by civil liberties groups and liberty-minded politicians.

Despite this, in the western world at least, online communications, especially social media, seemed to showcase classical liberal values of toleration, limited government and voluntary association. Free speech and (virtual) assembly flourished and opinions could be expressed in groups or to the world at large, subject only to the bounds of the general law and the conduct rules of the platform, unrestricted by state-sanctioned views of decency or suitability. This paper sets out how this situation is increasingly under threat, especially in the EU and the UK, as governments exercise increasing control over what is communicated online. They purport to adhere to liberal principles, by justifying measures in terms of harm prevention. But by defining harm to include being misled, distressed or offended, they are in danger of restricting the private sphere and free markets with little supporting evidence, doubtful prospects of success in countering genuinely harmful activity, and great risk of unintended consequences.

Measures have been pursued by EU institutions, parliamentary committees, government departments, charities, academics and media campaigns.

The breadth of the types of harms they wish to counter and of content that they wish to regulate is staggering. Disinformation, hate speech, electoral manipulation, microtargeting, trolling, bullying, offensive speech, child abuse, self-harm, terrorism, cybercrime, poor sleep quality, harassment – governments want to protect us from all of these and they have decided to enlist intermediaries to do it for them. These moves towards both regulating content and outsourcing responsibility for enforcement on to private providers are troubling and seem in many ways to be driven by a moral panic.

This paper focuses on two measures in particular: the UK government's Online Harms White Paper (soon to form the basis of an Online Safety Bill, expected to be announced in the May 2021 Queen's Speech) and the EU's Code of Practice on Disinformation. It goes on to consider how these developments affect, or are affected by, the established protections from liability for internet intermediaries, and the relationship between free markets and free speech online.

Legal but harmful

In the UK there are many laws and regulations that govern the lawfulness of speech – laws of defamation, negligence, malicious communications, laws relating to harassment, terrorism, child sexual exploitation. Some of these laws are investigated and enforced proactively by the authorities, to prevent publication of terrorist and extremist material, for example, and there have been growing efforts to harness the power of internet intermediaries as gatekeepers to identify and suppress illegal material at source.

Despite persistent rhetoric about the online world as a 'Wild West' of lawlessness,[1] a 2018 review by the Law Commission found that criminal laws apply equally, possibly more stringently, in the online world as offline. There are differences, both legal and practical, between how these laws apply in the online and offline worlds. In legal terms, under a longstanding EU law (Article 14 of the e-Commerce Directive[2]) internet platforms are not liable for unlawful content that they host unless they fail to remove it promptly when they are aware, or should have been aware, of it.[3] They also cannot be required to proactively monitor content posted by users, under Article 15 of the same directive. This distinguishes hosts of online content from publishers and creators. If platforms fail to remove content that they know about, they can be subject to criminal prosecution or civil action, which of course they can defend in the normal way and will eventually

1 For example, then Secretary of State for Digital, Culture, Media and Sport, Matt Hancock, declared in 2018 that 'the Wild West for tech companies is over' (https://www.telegraph.co.uk/technology/2018/03/18/wild-west-era-technology-firms-like-facebook-google-minister/)

2 Directive 2000/31/EC, at time of writing still applicable in the UK, carried into UK law at the end of the Transition Period.

3 Under the equivalent law in the US the so-called 'notice and take down' qualification does not apply. Under s.230 of the Communications Decency Act, platforms' immunity, other than in respect of copyright violations and federal criminal matters, is absolute.

only be liable if a court finds against them. In such cases all normal protections in law for freedom of expression and public interest apply. The outlook for this legal framework is considered further below.

In practical terms, however, the volume of content that is hosted and shared online, the relative absence of geographical or jurisdictional barriers to its dissemination and the possibility for anonymity, make general laws harder to enforce in the digital realm. There is a perception that these factors enable the commission of crimes and have caused an increase in offences such as terrorism and child abuse.

The proliferation of digital interactions beyond simply sharing static content into fast-moving interactive forums such as Twitter, and entertainment apps, has given rise to the UK government's concerns about wellbeing, especially that of children. The government has already used the vehicle of data protection law to empower the Information Commissioner to produce a Code of Practice on Age Appropriate Design[4] that will impose a duty on all operators of websites to act in the best interests of any child who may access their site. This means they must either make their site suitable for children or implement formal age controls to prevent children from accessing it. If they do not do so, the Information Commissioner may consider them to be in violation of data protection laws, with all the financial sanctions and reputational damage which this entails.

The Home Office and Department for Digital, Culture, Media and Sport (DCMS) have gone further, and wish to appoint a regulator, and platforms acting under codes of practice, as overseers of the personal wellbeing of adults and children. In 2019 the government published the Online Harms White Paper. In 2020 it published a response to the White Paper consultation and a final policy position. A draft 'Online Safety Bill' is expected in the course of 2021. The White Paper set out a regulatory framework to counter 'illegal and unacceptable content and activity', from terrorist plots and radicalisation to children's mental health and wellbeing; from child sexual abuse to 'echo chambers' and 'filter bubbles'; from gang culture to excessive screen time.

4 'Age appropriate design: a code of practice for online services', Information Commissioner's Office (https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/).

The framework will apply to 'companies that allow users to share or discover user-generated content or interact with each other online… including social media platforms, file hosting sites, public discussion forums, messaging services and search engines'. Service providers will be under a statutory duty of care 'overseen and enforced by an independent regulator'. The duty of care, as refined after the consultation, will be to 'improve safety for users of online services, and to prevent other people from being harmed as a direct consequence of content or activity on those services' (DCMS and Home Office 2020). While the White Paper provided examples of harm, such as bullying and undermining civil discourse, a definition of harm, or unacceptability, was deliberately omitted. The consultation response, however, conceded that 'a general definition of harmful content and activity would be provided', with 'priority categories' of harm to be set out in secondary legislation. It also appeared to limit the scope of 'harmful content' to only that which 'gives rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals'. While this seems to be an improvement on the original proposal, misinformation and disinformation are still considered to be in-scope harms, and content that is legal will still be subject to the duty of care.

The use of the expression 'duty of care' in the White Paper bears little resemblance to the concept as it currently exists in law. There is no precedent for such a general duty of care to prevent third parties from doing harm to each other. Creating a legal duty of care, whereby a platform could be held liable for actual damage suffered by individuals because of its actions or inaction would at least be legally consistent, but of course this is not the intention of the government. Proving loss or damage as a result of a breach of duty of care owed by a platform to a user is in reality likely to be impossible and would not capture all of the harms in the government's sights, or all of the people it wishes to protect.

As noted by leading lawyer Graham Smith in his response to the Online Harms Consultation, the creation of such a new type of duty will create a parallel legal system for online and offline content. It is likely to result in suppression of material that the UK Supreme Court has held[5] should not be suppressed, even if it would be distressing to a child reading it. It would also undermine the repeal of blasphemy laws (Smith 2019):

5 In Rhodes v OPO (2015) UKSC 32.

> The White Paper proposals would enable the regulator to deem blasphemous material to be harmful and to require intermediaries, as part of their duty of care, to take steps to restrict or, possibly, suppress it. Thus, by a sidewind, a deliberate decision of Parliament would be circumvented.

In practice this would mean that content that is legal in a book or newspaper could violate a regulator's code of practice against harmful material online. The online platform would be obliged to remove it or block it from being shared in the first place, but a book or newspaper publisher would not be restricted from publishing it.

Generations of lawmakers and judges have made and applied laws in ways that have sought to balance protecting lives, property and reputations against protecting free expression. This has not always been perfectly achieved and there are many laws that arguably infringe unduly on free speech.[6] Even then, perpetrators will have the right to defend themselves, evidentiary standards must be reached and prosecutors will take public interest considerations into account. Technology companies removing content at source by automated means, in order to protect themselves from censure by a regulator, will never be able to reflect this balance of interests.

While they contained assertions and assurances about free speech safeguards, the White Paper and the DCMS/Home Office response showed little sign that these vital legal points have been taken into account.

The enforcement powers proposed for the regulator included issuing fines and blocking access to non-compliant websites and apps. The possibility of personal liability for individuals is being held in reserve.

Which body can be expected to safeguard free speech and regulate material shared online? The Home Office and DCMS have confirmed that Ofcom will be the regulator of online harms. Ofcom is already the regulator of broadcast media. Recently, it has controversially censured broadcasters for a presenter's comments that 'risked undermining viewers' trust in advice from public authorities' and for exposing viewers to harm by interviewing conspiracy theorist David Icke (Ofcom 2020). Scaling up the powers and

6 For example, sending a communication that is indecent or grossly offensive is an offence under the Malicious Communications Act; displaying writing or other visible representation that is 'abusive' and likely to cause harassment, alarm or distress is an offence under the Public Order Act.

resources of this regulator to police the terms and conditions of, and content and behaviour on, platforms anywhere in the world that are visible in the UK does not augur well for freedom of expression and association.

In policy terms, it is the argument of this paper that the whole basis of the Online Harms agenda seems misplaced. There is little evidence that criminal activities are caused or exacerbated by the availability of internet platforms; if anything the internet has brought 'hypertransparency' to such activities. Rather than there being more harms and crimes in the world, they are more visible and this has given rise to a moral panic (Mueller 2015).

Some things that children are exposed to online, such as incitement to suicide and self-harm, and sharing of sexual imagery, are horrifying and harmful, but it does not follow that intermediaries should be responsible for countering these harms. A review of evidence for the Independent Inquiry into Child Sexual Abuse (CSA) found that (Wager et al. 2018):

> the online world is safe for most young people… Also, there is an increased familiarity with online risks and how to manage them among parents and young people. However there are gaps in the current understanding of the scale of online-facilitated CSA. There is a particular lack of evidence in relation to England and Wales, which restricts the accurate assessment of the scale of online-facilitated CSA in this country.

The Commons Science and Technology Committee considered that its 2018/2019 inquiry into the impact of social media and screen-use on young people's health had been **'**hindered by the limited quantity and quality of academic evidence available'. It was 'surprised to find that [the government] has not commissioned any new, substantive research to help inform its proposals [for new legislation]'.[7]

While it is difficult to prove that the prevalence of criminality and child abuse, as opposed to their visibility, has increased commensurately with the growth in online content sharing, it is in the interests of politicians and activist organisations in the field to claim causality. This justifies their claiming more power and influence over intermediaries and, indirectly, over us all. A better approach, in light of the increased visibility (which

7 Undeterred by the lack of evidence, the Committee considered that something must still be done and recommended sweeping regulatory interventions.

should surely assist in the investigation of such offences), would be to resource law enforcement and international efforts to investigate and punish the offenders (Aaronson et al. 2019). The Law Commission recommended reform of relevant criminal laws for clarity and effectiveness, and there may be a case for creating new criminal offences such as inciting a minor to suicide and self-harm. Sophisticated cross-border cooperation would be required for better investigation and enforcement, but this would equally be the case for enforcement of the proposed regulatory framework.

As to the prevention of nebulous categories of harm, there are good reasons why not everything that is harmful or undesirable is illegal. The state and its proxies intervening in such matters presents threats not just to freedom of expression but to the fundamentals of personal autonomy in a free society.

Disinformation and fake news

In Autumn 2018, the European Commission produced a Code of Practice on Disinformation.[8] It was entered into by technology companies and social media platforms, including Google, Facebook and Twitter. Disinformation was defined as:

> verifiably false or misleading information which (a) 'Is created, presented and disseminated for economic gain or to intentionally deceive the public'; and (b) 'may cause public harm', in turn defined as 'threats to democratic, political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security.'

Somewhat hopefully, it continued: 'The notion of "Disinformation" does not include misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary'. The way the Code has been applied in practice, however, shows that the idea of disinformation has been interpreted very broadly – arguably of necessity, since the volume of content that platforms have to moderate is vast and can only be overseen by automated means applying generalised rules.

Signatories agreed that there need to be safeguards against disinformation and that they should 'dilute the visibility of disinformation by improving the findability of trustworthy content' and 'facilitate content discovery and access to different news sources representing alternative viewpoints', presumably whether the user wants such content and viewpoints or not. They committed to investing in 'technological means to prioritise relevant,

8 'Code of Practice on Disinformation', European Commission (https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation).

authentic and authoritative information where appropriate in search, feeds or other automatically ranked distribution channels'.

The Code of Practice was prompted by widespread concerns (at least amongst establishment media and politicians) that democracies were being overrun with fake news and manipulative advertising by foreign powers and unscrupulous campaigners, leading unsuspecting, malleable viewers and readers to vote for Brexit and Donald Trump. In fact, there is little evidence that, for example, Russian bots or microtargeted campaign messaging had a defining influence on any election or vote (Bayer et al. 2017; Flynn et al. 2017). It is easier, though, for incumbent politicians to attribute the rise of populism to dark arts and manipulation (which they can then righteously seek to eliminate) than to any substantive concerns or political beliefs and values (which might require them to act to address the concerns or make the substantive case for their values). In this light, the anti-disinformation agenda pursued by the European Union, also reflected in the UK Online Harms White Paper, is troubling for both freedom of expression and the future of democracy. It also unbalances the legal regime that has so far governed the liability of intermediaries for third party content and that has allowed the digital economy to grow, as discussed further below.

Take, for example, the reliance placed by the Code of Practice on trusted fact-checkers as part of the effort to prioritise authoritative content. When subject matter may be highly contestable or unclear, a fact check will not always be useful in establishing whether content is right or wrong, misleading or harmful. Factcheckers are not themselves free of bias – in particular when they are approved by the government itself, as the Code of Practice envisages. This did not go unnoticed by President Trump. His fury at being 'factchecked' by Twitter (by reference to a news organisation that is widely considered to have adopted a political position of its own) provoked executive action that may cause the legal basis of platform liability in the US (and, as a result, across the world) to unravel.[9] Global technology companies are being mandated to filter and censor content by the authorities in Europe, and have been threatened with punitive action in the United States for doing so.

9 Executive Order on Preventing Online Censorship, 28 May 2020, seeks to 'clarify' that the immunity under section 230 should not extend to 'provide protection for those who purport to provide users a forum for free and open speech, but in reality use their power over a vital means of communication to engage in deceptive or pretextual actions stifling free and open debate by censoring certain viewpoints'.

Signatories to the Code of Practice may have hoped that by enthusiastically joining in a voluntary process, they would stave off the possibility of formal regulation. If so they seem likely to be disappointed. The EU's Justice Commissioner told the European Parliament in May 2020 that the experience of the Covid-19 pandemic showed the need for regulation to enable the Commission to go further in working with platforms to 'remove messages from social media'.

The impossibility of policing disinformation fairly and without prejudicing free speech was illustrated in the course of the 2020 Covid-19 outbreak. Videos carrying critical discussions of government policies were suppressed by YouTube, while the BBC on occasion carried highly misleading statistics with impunity. This is not a call for the BBC to be factchecked and down-rated for untrustworthy content, but these cases illustrate the inconsistencies and biases that are in play and the impossibility of definitively determining and pronouncing on the reliability of information. A free and open debate on contentious matters, even, or perhaps especially, difficult and technical subjects, is vital to reach the truth and for the truth to be widely believed. State-mandated suppression of conspiracy theories will not eliminate these theories but will rather lend them credibility in some eyes.

Rowing back from safe harbours

Social media platforms are private operators and therefore not bound to respect the freedom of expression of users. They are entitled to implement whatever fact-checking and moderation policies they see fit. But, as illustrated by the examples above, governments are intervening to force or coerce private operators into limiting free speech on their platforms. This is a reverse of the aims of the legal 'safe harbours' that have underpinned the development of the digital economy.

For twenty years the European Union's e-Commerce Directive has required that service providers who merely host content will not be liable for unlawful material, unless they had knowledge of it and failed to remove it. The UK government had announced[10] an intention to review these existing liability frameworks to make them 'work better'. It appears though, according to the Online Harms White Paper, that it decided against this, for now. The White Paper posited that new *ex ante* regulation will deliver a balance between 'existing law that enables platforms to operate' and increased responsibilities to maintain processes and governance to 'reduce the risk of illegal and harmful activity'.

Under the Directive, platforms can already be liable for content where they have gone beyond passive hosting, and there is a body of case law where this has happened. So, the Online Harms framework and Code of Practice on Disinformation themselves may not transgress Article 14 of the European Convention on Human Rights directly, but they seem to mandate the platforms to act in ways that could take them outside of the immunity. Platforms risk not only being penalised by regulators for allowing 'harmful' or 'unacceptable' content to be shared, but also becoming liable

10 In a speech by Theresa May at the World Economic Forum in Davos, January 2018.

under the general law as a result of their efforts to comply with regulation. All of this will have serious effects on free speech online, illustrating the reasons for the liability safe harbours in the first place.[11]

It is widely believed that liability safe harbours were introduced around the world to nurture the development of internet services or to prevent the inequity of liability for material outside their control. Technology companies would certainly have lobbied for and welcomed them for this reason. But the immunities from liability also brought wider social benefits. Platforms were not to be treated as creators, speakers or publishers because the liability that attaches to those roles in law would have incentivised them to remove and filter content that may be lawful, but is not worth the risk to the platform of carrying it. The interests and incentives of platforms and users diverge. Without immunity from liability for material produced by others, platforms would filter lawful content that creators themselves would be content to publish at their own risk. This 'collateral censorship' would result in the loss of content that is beneficial to society (Wu 2011). European governments today seem to believe that the benefits of free circulation and exchange of information and ideas are outweighed by the potential harmfulness, unacceptability or illegality of some of them. What had been seen as the dangers of collateral censorship are now seen as a benefit, or a tool for government to exercise control of online speech through the intermediaries.

Arguments for reviewing the liability safe harbours because social media platforms can and do control content that they host, are seductive. Why should they benefit from (extremely valuable) protection from liability that traditional publishers do not have? But withdrawing the immunity after large platforms have benefited from it for decades, building their models without the legal and regulatory costs of liability for user content, risks entrenching the current dominant social media operators, stifling the ability of smaller and newer competitors to grow under similarly benign conditions. Retaining the favourable legal immunities but adding *ex ante* regulation seems likely to deliver a worst-of-all-worlds outcome: aggressive filtering and censorship through use of costly technologies and human resources that will create barriers to entry for new platforms and technologies, while incumbent platforms can absorb these costs and continue to enjoy the established protections from *ex post* liability.

11 The recitals to the Directive reference the 'free movement of information society services' as 'a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) [of the ECHR]'.

Free speech needs free enterprise

Restrictions on free speech that will result from regulations such as those in place or being developed in the UK and EU are arguably more damaging than rules established by platforms acting autonomously. Platforms can have different policies and serve different audiences, so having individual platforms that are restrictive in their moderation does not necessarily have an adverse effect on freedom of expression. However, there could be serious adverse effects on free speech if the state intervenes to require all platforms to restrict content in furtherance of government policy, or threatens regulation such that platforms proactively do so to seem cooperative and be involved in shaping regulation to suit their interests.

Outsourcing the enforcement of restrictions to private operators will likely mean that private operators will act to restrict and filter 'harmful' content in ways that suit their commercial and private interests without accountability for policy implications. They will have to rely on automated means to do so. They will not have the incentive or the capacity to consider all the defences and mitigations that might be available in respect of a piece of content. And they will have their own political biases. It may be possible to make such private operators more transparent and open in their decision making, and even appoint some kind of ombudsman to oversee that it is operated fairly,[12] but that would erode further the private rights of individuals to run their businesses and require yet more regulation.

12 As put forward for example by Professor Lilian Edwards in evidence to the House of Lords Select Committee inquiry into the regulation of the internet and the Santa Clara Principles, published in 2018 by a group of organisations, advocates, and academic experts who support the right to free expression online.

Having intermediaries filter content to enforce law and policy is popular with governments and intellectual property rightsholders as it is considered to be a low-cost approach to addressing content that is illegal (or simply undesirable) posted by thousands of, often unidentifiable, users. However, outsourcing compliance in this way comes with costs of its own. Illegality is hard to identify with certainty; harmfulness and acceptability, impossible. False positives will abound. Collateral censorship and monitoring of individuals (in tension with privacy and data protection laws) will be the norm. This is already the direction of travel under instruments such as the EU Communication on Illegal Content from 2017 and the Netz-DG[13] in Germany: automated solutions are encouraged and success is judged by takedown rates, favouring volume and speed over nuance.

13 The Network Enforcement Act which came into force in 2018 requires social media providers to remove 'obviously' illegal content within 24 hours and other illegal content within seven days or be fined up to €50 million.

A fool's errand?

While the endeavour to eliminate disinformation and harm from the internet seems likely to be a fool's errand, great damage could be done in the process. The emphasis on harm reduction 'by design' in the Online Harms White Paper and the Code of Practice on Disinformation hints at the hubris that underlies them. The idea that IT and compliance professionals simply need to apply their skills and foresight to design away harm, and that they will do so in ways that respect freedom of expression and are free from bias, under a regulator capable of monitoring the compliance of potentially every interactive platform in the world, is almost laughable. It is also naïve to think that the technical capabilities that platforms will deploy and the powers that governments will accrue will be always used respectfully, even in liberal democracies. Such regulations can be used in partisan ways: claiming that a political or philosophical opponent's words are harmful or unacceptable will be used as a tool to obstruct or silence them. Western governments used to express disapproval at censorship of the internet by authoritarian regimes; now they seem to be suggesting it is a moral duty of the state.

The assumption by the authorities that they know what is harmful or unacceptable and have a duty to protect people from it is itself authoritarian. The idea that adults need government guidance and protection to prevent them from being offended or exploited by 'purveyors of disinformation', or that governments and social media platforms are in a better position than parents to supervise screen time and content for children, is unsettling. It will be counterproductive if parents come to believe that the internet has been made safe for children and less supervision is required. If ministers and campaigners consider that parents are not exercising enough supervision and control of children's lives online at present, the online harms framework will make that worse (potentially resulting in a cycle of ever stricter measures). Governments should surely be wary of such

incursion into homes and private lives if they wish to claim to be defenders of personal responsibility and the family.

The UK and the EU are taking great risks in moving towards content regulation. Measures such as those discussed in this paper are unlikely to reduce harm or protect democracy, but could mean losses in trust in institutions, and reductions in freedom of expression and association. There will be economic costs if innovation and competition suffer and the vast consumer surplus from digital services dissipates. Measures such as age verification and requirements to make content suitable for children will make online services less useful. Not being able freely to express and receive ideas and information is itself a harm. It is a huge price to pay for authorities being unable to take responsibility for law enforcement, reconcile to losing political battles or trust people to be able to make decisions for themselves and their families.

References

Aaronson, S. A. and others, Academics and Civil Society Organizations (2019) Liability for User-Generated Content Online, Principles for Lawmakers. *Santa Clara Law Digital Commons* (https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2992&context=historical).

Bayer, J., Bitiukova, N., Szakács, J., Alemanno, A. and Uszkiewicz, E. (2017) Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. Report to European Parliament (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf).

Department for Digital, Culture, Media and Sport (2019) Code of Practice for providers of online social media platforms (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973937/Code_of_Practice_for_providers_of_online_social_media_platforms.d_V2.pdf).

Edwards, L. (2018) Evidence to House of Lords Select Committee on Communications inquiry into the regulation of the internet (https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf).

European Commission (2017) Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms (https://digital-strategy.ec.europa.eu/en/library/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms).

European Commission (2018) Code of Practice on Disinformation (https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation).

Flynn, D. J., Nyhan, B. and Reifler, J. (2017) The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics. *Political Psychology* 38(S1): 127-150.

Home Office and Department for Digital, Culture, Media and Sport (2019) Online Harms White Paper (https://www.gov.uk/government/consultations/online-harms-white-paper).

House of Commons Science and Technology Committee (2019) Impact of social media on screen-use on young people's health (https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/822/822.pdf).

Law Commission (2018) Scoping Report on Abusive and Offensive Online Communications (https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/).

Mueller, M. L. (2015) Hyper-transparency and social control: social media as magnets for regulation. *Telecommunications Policy* 39(9): 804-810.

Ofcom (2020) Decisions on recent programmes featuring David Icke and Eamonn Holmes (https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/david-icke-and-eamonn-holmes-decision).

Smith, G. (2019) Online Harms White Paper - Response to Consultation (https://www.cyberleagle.com/2019/06/speech-is-not-tripping-hazard-response.html).

Wager, N., Armitage, R., Christmann, K., Gallagher, B., Ioannou, M., Parkinson, S., Reeves, C., Rogerson, M. and Synnott, J. (2018) Rapid Evidence Assessment Quantifying the Extent of Online Facilitated Child Sexual Abuse. Report for the Independent Inquiry into Child Sexual Abuse (https://www.iicsa.org.uk/document/rapid-evidence-assessment-quantifying-extent-online-facilitated-child-sexual-abuse).

Wu, F. T. (2011) Collateral Censorship and the Limits of Intermediary Immunity. *Notre Dame Law Review* 87(1): 293.

The Institute of Economic Affairs
2 Lord North Street
London SW1P 3LB
Tel 020 7799 8900
email iea@iea.org.uk